| APPLICATION NO. | FILING DATE | FIRST NAMED INVENTOR | ATTORNEY DOCKET NO. | CONFIRMATION NO. |
|---|---|---|---|---|
| 09/707,702 | 11/07/2000 | Paul W. Dent | 1280.00272 | 9559 |

| | |
|---|---|
| 7590     06/15/2004 | |

David E Bennett
COATS & BENNETT
1400 Crescent Green
Suite 300
Cary, NC 27511

| EXAMINER |
|---|
| CHEN, SHIN HON |

| ART UNIT | PAPER NUMBER |
|---|---|
| 2131 | 6 |

DATE MAILED: 06/15/2004

Please find below and/or attached an Office communication concerning this application or proceeding.

| | Application No. | Applicant(s) |
|---|---|---|
| **Office Action Summary** | 09/707,702 | DENT ET AL. |
| | Examiner | Art Unit |
| | Shin-Hon Chen | 2131 |

*-- The MAILING DATE of this communication appears on the cover sheet with the correspondence address --*

**Period for Reply**

A SHORTENED STATUTORY PERIOD FOR REPLY IS SET TO EXPIRE _3_ MONTH(S) FROM
THE MAILING DATE OF THIS COMMUNICATION.
- Extensions of time may be available under the provisions of 37 CFR 1.136(a). In no event, however, may a reply be timely filed
  after SIX (6) MONTHS from the mailing date of this communication.
- If the period for reply specified above is less than thirty (30) days, a reply within the statutory minimum of thirty (30) days will be considered timely.
- If NO period for reply is specified above, the maximum statutory period will apply and will expire SIX (6) MONTHS from the mailing date of this communication.
- Failure to reply within the set or extended period for reply will, by statute, cause the application to become ABANDONED (35 U.S.C. § 133).
  Any reply received by the Office later than three months after the mailing date of this communication, even if timely filed, may reduce any
  earned patent term adjustment. See 37 CFR 1.704(b).

**Status**

1)☒ Responsive to communication(s) filed on *13 August 2002*.

2a)☐ This action is **FINAL**.    2b)☒ This action is non-final.

3)☐ Since this application is in condition for allowance except for formal matters, prosecution as to the merits is
closed in accordance with the practice under *Ex parte Quayle*, 1935 C.D. 11, 453 O.G. 213.

**Disposition of Claims**

4)☐ Claim(s) _____ is/are pending in the application.

  4a) Of the above claim(s) _____ is/are withdrawn from consideration.

5)☐ Claim(s) _____ is/are allowed.

6)☒ Claim(s) *1-50* is/are rejected.

7)☐ Claim(s) _____ is/are objected to.

8)☐ Claim(s) _____ are subject to restriction and/or election requirement.

**Application Papers**

9)☐ The specification is objected to by the Examiner.

10)☒ The drawing(s) filed on *07 November 2000* is/are: a)☒ accepted or b)☐ objected to by the Examiner.

  Applicant may not request that any objection to the drawing(s) be held in abeyance. See 37 CFR 1.85(a).

  Replacement drawing sheet(s) including the correction is required if the drawing(s) is objected to. See 37 CFR 1.121(d).

11)☐ The oath or declaration is objected to by the Examiner. Note the attached Office Action or form PTO-152.

**Priority under 35 U.S.C. § 119**

12)☐ Acknowledgment is made of a claim for foreign priority under 35 U.S.C. § 119(a)-(d) or (f).

  a)☐ All  b)☐ Some * c)☐ None of:

    1.☐ Certified copies of the priority documents have been received.

    2.☐ Certified copies of the priority documents have been received in Application No. _____.

    3.☐ Copies of the certified copies of the priority documents have been received in this National Stage
    application from the International Bureau (PCT Rule 17.2(a)).

  * See the attached detailed Office action for a list of the certified copies not received.

**Attachment(s)**

1)☒ Notice of References Cited (PTO-892)
2)☐ Notice of Draftsperson's Patent Drawing Review (PTO-948)
3)☒ Information Disclosure Statement(s) (PTO-1449 or PTO/SB/08)
  Paper No(s)/Mail Date *2 and 5*.

4)☐ Interview Summary (PTO-413)
  Paper No(s)/Mail Date. _____ .
5)☐ Notice of Informal Patent Application (PTO-152)
6)☐ Other: _____.

## DETAILED ACTION

1.      Claims 1-50 have been examined.

### *Claim Rejections - 35 USC § 102*

2.      The following is a quotation of the appropriate paragraphs of 35 U.S.C. 102 that form the

basis for the rejections under this section made in this Office action:

> A person shall be entitled to a patent unless –
>
> (e) the invention was described in (1) an application for patent, published under section 122(b), by another filed
> in the United States before the invention by the applicant for patent or (2) a patent granted on an application for
> patent by another filed in the United States before the invention by the applicant for patent, except that an
> international application filed under the treaty defined in section 351(a) shall have the effects for purposes of this
> subsection of an application filed in the United States only if the international application designated the United
> States and was published under Article 21(2) of such treaty in the English language.

3.      Claims 1, 2, 4, 5, 6, 17, 18, 120, 21, 22, 33, 34, 35, 37, 48, 49, and 50 are rejected under

35 U.S.C. 102(e) as being clearly anticipated by Kocher et al. U.S. Pat. No. 6327661 (hereinafter

Kocher).

4.      As per claim 1, 17, and 34, Kocher discloses in a computational device for performing

secret cryptographic calculations with secret numbers, a method of hiding secret information

from outside observation comprising: scheduling said calculations using a precomputed, fixed

randomization schedule in such a way that externally observable parameters of the device cannot

be associated to particular pieces, bits, symbols or values of said secret information (Kocher:

column 1 line 64 – column 2 line 52).

5.      As per claim 2,18, and 35, Kocher discloses the method of claims 1, 17, and 34

respectively. Kocher further discloses in which scheduling said calculations comprises inserting

dummy calculations according to a schedule associated with one of said secret numbers in the middle of calculations using the associated secret number (Kocher: column 1 line 64 – column 2 line 52).

6.    As per claim 4, 20, and 37, Kocher discloses the method of claims 2, 18, and 35 respectively. Kocher further discloses in which said dummy calculations affect a pattern of variation of power supply current consumed by the device so as to mask any correlation between power supply current variation and said secret information (Kocher: column 1 line 64 – column 2 line 52).

7.    As per claim 5 and 21, Kocher discloses the method of claims 1 and 17 respectively. Kocher further discloses in which said externally observable parameters include variation in power supply current (Kocher: column 1 line 64 – column 2 line 52).

8.    As per claim 6 and 22, Kocher discloses the method of claim 1 and 17 respectively. Kocher further discloses in which said externally observable parameters include variation in timing of outputting results of said calculations (Kocher: column 1 line 64 – column 2 line 52).

9.    As per claim 33, Kocher discloses the device of claim 17. Kocher further discloses wherein device comprises a smart card (Kocher: column 14 lines 6-59).

10.    As per claim 48, Kocher discloses the mobile terminal of claim 34. Kocher further discloses wherein said device comprises a smart card (Kocher: column 14 lines 6-59).

11.    As per claim 49, Kocher discloses the mobile terminal of claim 34. Kocher further

discloses wherein said device comprises a subscriber identity module (Kocher: column 14 lines

6-59).

12.    As per claim 50, Kocher discloses the mobile terminal of claim 34. Kocher further

discloses wherein said secret number comprises a private cryptographic key (Kocher: column 1

line 64 – column 2 line 52).

### *Claim Rejections - 35 USC § 103*

13.    The following is a quotation of 35 U.S.C. 103(a) which forms the basis for all

obviousness rejections set forth in this Office action:

> (a) A patent may not be obtained though the invention is not identically disclosed or described as set forth in
> section 102 of this title, if the differences between the subject matter sought to be patented and the prior art are
> such that the subject matter as a whole would have been obvious at the time the invention was made to a person
> having ordinary skill in the art to which said subject matter pertains.  Patentability shall not be negatived by the
> manner in which the invention was made.

14.    Claims 3, 19, and 26 are rejected under 35 U.S.C. 103(a) as being unpatentable over

Kocher in view of Messerges et al. U.S. Pat. No. 6298135 (hereinafter Messerges) and further in

view of Ohki et al. U.S. Pat. No. 6408075 (hereinafter Ohki).

15.    As per claim 3, 19, and 36,  Kocher discloses the method of claims 2, 18, and 35

respectively. Kocher does not explicitly disclose in which the schedule uses a randomizing

indicator in the form of a binary word having a length equal to that of the secret number and

having a binary one in a select number of places that the secret number has a binary zero.

However, AAPA discloses using modular exponentiation based on corresponding bit value as

cryptographic function (Messerges: column 3 line 39 – column 4 line 51). Therefore, it would have been obvious to one having ordinary skill in the art to combine the teachings of Messerges within the system of Kocher because it is well known in the art to randomize modular exponentiation (RSA) as cryptographic function.

Kocher as modified does not explicitly disclose uses a randomizing indicator in the form of a binary word having a length equal to that of the secret number and having a binary one in a select number of places that the secret number has a binary zero. However, Ohki discloses using bit inverted data to cause randomization of calculation (Ohki: column 2 line 38 – column 5 line 12). It would have been obvious to one having ordinary skill in the art to combine the teachings of Ohki within the combination of Kocher-Messerges because it increases security of the system by reducing the correlation between the secret number and the current.

16.     Claims 7-10, 23-26, and 38-41 are rejected under 35 U.S.C. 103(a) as being unpatentable over Kocher in view of Messerges.

17.     As per claim 7, 23, and 38, Kocher discloses the method of claims 1, 17, and 34 respectively. Kocher does not explicitly disclose in which said secret cryptographic calculations comprise exponentiating a long integer to the power of a large secret exponent. However, Messerges discloses that limitation (Messerges: column 3 line 39 – column 4 line 51). It would have been obvious to one having ordinary skill in the art to combine the teachings of Messerges within the system of Kocher because it is well known in the art to use modular exponentiation (RSA) as cryptographic function.

18.     As per claim 8, 24, and 39, Kocher as modified discloses the method of claims 7, 23, and

38 respectively. Kocher as modified further discloses in which exponentiating a long integer to

the power of a large secret exponent comprises forming successive squares of said long integer

reduced modulo a given modulus (Messerges: column 3 line 39 – column 4 line 51).

19.     As per claim 9, 25, and 40, Kocher as modified discloses the method of claims 8, 24, and

39 respectively. Kocher as modified further discloses in which successive squares are performed

in groups of a fixed length and the results temporarily stored (Messerges: column 3 line 39 –

column 4 line 51).

20.     As per claim 10, 26, and 41, Kocher as modified discloses the method of claims 9, 25,

and 40 respectively. Kocher as modified further discloses the method comprising selecting to

multiplicatively accumulate certain ones of said stored results dependent on if corresponding bits

of one of said secret exponents is binary one or binary zero in such a way that the stored results

which are selected cannot be determined from outside said device (Messerges: column 3 line 39

– column 4 line 51).

21.     Claims 11-13, 27-29, and 42-44 are rejected under 35 U.S.C. 103(a) as being

unpatentable over Kocher in view of Applicant's Admitted Prior Art (hereinafter AAPA).

22.     As per claim 11, 27, and 42, Kocher discloses the method of claims 1, 17, and 34

respectively. Kocher does not explicitly disclose scheduling said calculations in such a way as to

reduce computational effort. However, AAPA discloses that using modular exponentiation

reduces the effort in raising a large number (AAPA: page 3 lines 3-17). It would have been obvious to one having ordinary skill in the art to combine the teachings of AAPA within the system of Kocher because it is well known in the art to use modular exponentiation to reduce computational effort.

23.     As per claim 12, 28, 43, Kocher as modified discloses the method of claims 11, 27, and 42 respectively. Kocher as modified further discloses in which said calculations include exponentiating a long integer to the power of a large secret exponent (AAPA: pages 2-3).

24.     As per claim 13, 29, and 44, Kocher as modified discloses the method of claims 12, 28, and 43 respectively. Kocher as modified further discloses in which said large secret exponent is generated upon first commissioning said device into operation and is internally stored and never released outside the device (AAPA: page 2 lines 17-19).

25.     Claims 14, 30, and 45 are rejected under 35 U.S.C. 103(a) as being unpatentable over Kocher in view of AAPA and further in view of Ohki.

26.     As per claims 14, 30, and 45, Kocher as modified discloses the method of claims 12, 28, and 43 respectively. Kocher as modified does not explicitly disclose in which said secret exponent is factorized into a product of sparse integers plus a remainder such that the total number of ones in a binary representation of said sparse integers and said remainder is a minimum. However, Ohki discloses making the number of '0' to '1' or vice versa transition constant as to reduce the current consumption (Ohki: column 2 line 38 – column 5 line 12). It

would have been an obvious matter of design choice to modify the Ohki reference to make total

number of ones in a binary representation of said sparse integers and said remainder minimum,

since the applicant does not disclose that making total number of ones in a binary representation

of said sparse integers and said remainder minimum solves any stated problem or is for particular

purpose, and it appears that by making the transition of '0' to '1' or vice versa constant would

work equally well.

27.     Claims 15, 16, 31, 32, 46, and 47 are rejected under 35 U.S.C. 103(a) as being

unpatentable over Kocher in view of AAPA and further in view of Lin et al. U.K. Pat. No.

2345229 (hereinafter Lin)

28.     As per claim 15, 31, and 46, Kocher as modified discloses the method of claims 13, 29,

and 44 respectively. Kocher as modified does not explicitly disclose the method further

comprising generating in association with said secret exponent and storing in association

therewith a precomputed pseudorandom schedule of dummy calculations to be inserted amidst

calculations using said secret exponent. However, Lin discloses that limitation (Lin: abstract and

pages 4 and 11). It would have been obvious to one having ordinary skill in the art to combine

the teachings of Lin within the combination of Kocher-AAPA because it increases the security

by enforcing randomization and dummy calculations insertion.

29.     As per claim 16, 32, and 47, Kocher as modified discloses the method of claims 15, 31,

and 46 respectively. Kocher as modified further discloses said schedule of dummy calculations

comprises dummy multiplications associated with a small fraction of the bits of said exponent

which are equal to one particular binary bit polarity (AAPA: page 3 lines 3-17 and Lin: abstract and pages 4 and 11). It would have been obvious to one having ordinary skill in the art to combine the teachings of Kocher, AAPA, and Lin because it increases the security by enforcing randomization and dummy calculations insertion and randomize calculation based on bit value.

## *Conclusion*

30.     The prior art made of record and not relied upon is considered pertinent to applicant's disclosure.

Odinak U.S. Pat. No. 6419159 discloses integrated circuit device with power analysis protection circuitry.

Singer U.S. Pat. No. 6724894 discloses cryptographic device having reduced vulnerability to side-channel attack and method of operating same.

Any inquiry concerning this communication or earlier communications from the examiner should be directed to Shin-Hon Chen whose telephone number is (703) 305-8654. The examiner can normally be reached on Monday through Friday 8:30am to 5:30pm.

If attempts to reach the examiner by telephone are unsuccessful, the examiner's supervisor, Ayaz Sheikh can be reached on (703) 305-9648. The fax phone number for the organization where this application or proceeding is assigned is 703-872-9306.

Information regarding the status of an application may be obtained from the Patent

Application Information Retrieval (PAIR) system.  Status information for published applications

may be obtained from either Private PAIR or Public PAIR.  Status information for unpublished

applications is available through Private PAIR only.  For more information about the PAIR

system, see http://pair-direct.uspto.gov. Should you have questions on access to the Private PAIR

system, contact the Electronic Business Center (EBC) at 866-217-9197 (toll-free).

Shin-Hon  Chen
Examiner
Art Unit 2131

SC

AYAZ SHEIKH
SUPERVISORY PATENT EXAMINER
TECHNOLOGY CENTER 2100